FortiWeb for Microsoft Azure Quick Start Guide

FORTIWEB FOR MICROSOFT AZURE QUICK START GUIDE

The following section will take you through a step-by-step process in order to deploy Fortinet FortiWeb on Azure.

What is Fortinet FortiWeb for Azure?

Unprotected web applications are the easiest point of entry for hackers and vulnerable to a number of attack types. Our multi-layered and correlated approach protects your web apps from the Open Web Application Security Project (OWASP) Top 10 and more. Our Web Application Security Service from FortiGuard Labs uses information based on the latest application vulnerabilities, bots, suspicious URL and data patterns, and specialized heuristic detection engines to keep your applications safe from:

Malicious Sources

- Denial-of-service (DoS) attacks
- Sophisticated threats such as SQL injection, cross-site scripting, buffer overflows, and cookie poisoning
- Malware uploads and application distributed denial-of-service (DDoS) and other attacks

It also includes Layer 7 load balancing and accelerated SSL offloading for more efficient application delivery.

The FortiWeb Web Application Firewall (WAF) provides nearly 100% protection from even the most sophisticated attacks with:

- Vulnerability scanning
- IP reputation, attack signatures, and antivirus powered by FortiGuard
- Behavioral attack detection, threat scanning, protection against botnets, DDoS, automated attacks, and more
- Integration with FortiSandbox for advanced threat protection (ATP) detection
- Tools to give you valuable insights on attacks
- Available in the Azure Marketplace

Why Fortinet FortiWeb on Azure?

Web Application Firewalls

Web Applications Are an Easy Target

Although Payment Card Industry Data Security Standard (PCI DSS) compliance is the main reason most organizations deploy web application firewalls (WAFs), many now realize that unprotected web applications are the easiest point of entry for even unsophisticated hackers. Externally facing web applications are vulnerable to attacks such as cross-site scripting, SQL injection, and Layer 7 DoS. Internal web applications are even easier to compromise if an attacker is able to gain access to an internal network where many organizations think they're protected by their perimeter network defenses. Custom code is usually the weakest link as development teams have the impossible task of staying on top of every new attack type. However, even commercial code is vulnerable as many organizations don't have the resources to apply patches and security fixes as soon as they're made available. Even if you apply every patch and have an army of developers to protect your systems, zero-day attacks can leave you defenseless and only able to respond after the attack has occurred.

Comprehensive Web Application Security with FortiWeb

Using an advanced multi-layered and correlated approach, FortiWeb provides complete security for your external and internal web-based applications from the OWASP Top 10 and many other threats. Using IP reputation services, botnets and other malicious sources are automatically screened out before they can do any damage. DoS detection and prevention keep your applications safe from being overloaded by Layer 7 DoS attacks. FortiWeb checks that the request hasn't been manipulated using HTTP RFC validation. Requests are checked against FortiWeb's signatures to compare them against known attack types to make sure they're clean. Any files, attachments, or code are scrubbed with FortiWeb's built-in antivirus and anti-malware services. FortiWeb's auto-learning behavioral detection engine reviews all requests that have passed the tests for known attacks. If the request is outside of user or automatic parameters, the request is blocked. Lastly, FortiWeb provides a correlation engine where multiple events from different security layers are correlated to make a more accurate decision and help protect against the most sophisticated attacks. This combination provides nearly 100% protection from any web application attacks, including zero-day threats that signature file-based systems can't detect.

Included Vulnerability Scanning

Only FortiWeb includes a web application vulnerability scanner in every appliance at no extra cost to help you meet PCI DSS compliance. FortiWeb's vulnerability scanning dives deep into all application elements and provides in-depth results of potential weaknesses in your applications. Vulnerability scanning is always up to date with regular updates from FortiGuard Labs.

Deep Integration with FortiGate and FortiSandbox

As the threat landscape evolves, many new threats require a multi-pronged approach for protecting web-based applications. Advanced persistent threats that target users can take many different forms than traditional single-vector attack types and can evade protections offered only by a single device. FortiWeb's integration with FortiGate and FortiSandbox extend basic WAF protections through synchronization and sharing of threat information to both deeply scan suspicious files and share infected internal sources.

FortiWeb is one of many Fortinet products that provide integration with our FortiSandbox advanced threat detection platform. FortiWeb can be configured with FortiSandbox to share threat information and block threats as they're discovered in the sandboxing environment. Files uploaded to web servers can be sent to FortiSandbox and FortiSandbox Cloud for analysis. Alerts are sent immediately when malicious files are identified and future similar files are blocked immediately.

Integration with FortiGate enables the sharing of quarantined IP addresses detected and maintained on the FortiGate firewall. Through regular polling of the FortiGate, FortiWeb is up to date with the latest list of internal sources that have or are suspected of being infected and blocks traffic from these devices to prevent more damage.

Additionally, FortiGate users can now simplify the deployment of FortiWeb in a Fortinet-based network. Using the WCCP protocol, a FortiGate can be configured to direct HTTP traffic for inspection to a FortiWeb without having to manually configure routers or DNS services. Users can set up custom rules to route specific traffic using comprehensive, granular forwarding policies.

Advanced False Positive Mitigation Tools with User Scoring and Session Tracking

False positive detections can be very disruptive if a web application firewall isn't configured correctly. Although the installation of a WAF may take only minutes, fine-tuning it to minimize false positives can take days or even weeks. Plus, there's the regular ongoing adjustments for application and environmental changes. FortiWeb combats this problem with many sophisticated tools including alert tuning, white lists, automatic learning exceptions, correlated threat detection, and advanced code-based syntax analysis.

FortiWeb is the only WAF that employs user scoring and session tracking to further enhance our false positive mitigation tools. Administrators can attach threat levels to any of FortiWeb's WAF protections, then set trigger thresholds that can block, report, or monitor users that cross a combined multi-event violation score over the lifetime of their session. Never before has this level of customization and advanced correlation been available in a WAF, and it can dramatically reduce the number of false positive detections depending on the level of sensitivity set by the administrator.

FortiWeb User Tracking

FortiWeb monitors users authenticating to web applications and tracks all their subsequent activity. All traffic and attack logs are attached with the username, allowing rule enforcement and forensics at the user level.

Secured by FortiGuard

Fortinet's award-winning FortiGuard Labs is the backbone for many of FortiWeb's layers in its approach to application security. Offered as three separate options, you can choose the FortiGuard services you need to protect your web applications. FortiWeb IP Reputation Service protects you from known attack sources like botnets, spammers, anonymous proxies, and sources known to be infected with malicious software. FortiWeb Security Service is designed just for FortiWeb including items such as application layer signatures, malicious robots, suspicious URL patterns, and web vulnerability scanner updates. Finally, FortiWeb offers FortiGuard's top-rated antivirus engine that scans all file uploads for threats that can infect your servers or other network elements.

Virtual Patching

FortiWeb provides integration with leading third-party vulnerability scanners including Acunetix, HP WebInspect, IBM AppScan, Qualys, and WhiteHat to provide dynamic virtual patches to security issues in application environments. Vulnerabilities found by the scanner are quickly and automatically turned into security rules by FortiWeb to protect the application until developers can address them in the application code.

Blazing Fast SSL Offloading

FortiWeb is able to process up to tens of thousands of web transactions by providing hardware-accelerated SSL offloading in most models. With near real-time decryption and encryption using ASIC-based chipsets, FortiWeb can easily detect threats that target secure applications.

Application Delivery and Authentication

FortiWeb provides advanced Layer 7 load balancing and authentication offload services. FortiWeb can easily expand your applications across multiple servers using intelligent, application-aware Layer 7 load balancing and can be combined with SSL offloading for load balancing secure application traffic. Using HTTP compression, FortiWeb can also improve bandwidth utilization and user response times for content-rich applications. Authentication offloading integrates with many authentication services including LDAP, NTLM, Kerberos, and RADIUS with two-factor authentication for RADIUS and RSA SecurID. Using these authentication services, you can easily publish websites and use single sign-on (SSO) for any web application including Microsoft applications such as Outlook Web Access and SharePoint. Finally, FortiWeb can improve application response times by caching often-used content to serve it to users faster than having to request the same information each time it is needed.

VM and Cloud Options

FortiWeb provides maximum flexibility in supporting your virtual and hybrid environments. The virtual versions of FortiWeb support all the same features as our hardware-based devices and work with all the top hypervisors including VMware, Microsoft Hyper-V, Citrix XenServer, Open Source Xen, and KVM. FortiWeb is also available for Amazon Web Services and Microsoft Azure.

Central Management and Reporting

FortiWeb offers the tools you need to manage multiple appliances and gain valuable insights on attacks that target your applications. From within a single management console you can configure and manage multiple FortiWeb gateways using our VMware-based central management utility. If you need an aggregated view of attacks across your network, FortiWeb easily integrates into our FortiWeb reporting appliances for centralized logging and report consolidation from multiple FortiWeb devices.

How to Deploy Fortinet FortiWeb in Microsoft Azure Using the Azure Portal

The Fortinet FortiWeb for Microsoft Azure is deployed as a virtual machine in Microsoft's Azure cloud (IaaS). You will see in the following sections how we deploy and configure the Fortinet FortiWeb in the Azure Marketplace.

- Fortinet FortiWeb 14-Day Trial
- Fortinet FortiWeb (BYOL)—This is currently the only licensing model that is supported. Fortinet also offers a 60-day evaluation license.

BEFORE YOU GET STARTED

Before you can being to deploy Fortinet's FortiWeb for Azure, you will need to make sure the following conditions have been met in order to successfully complete the installation:

- Create a Microsoft Azure account
- Obtain a license (choose one of the following):
    1. Purchase a Fortinet FortiWeb license for Microsoft Azure http://www.windowsazure.com/en-us/account/
    2. Register to receive an evaluation license from the Fortinet website

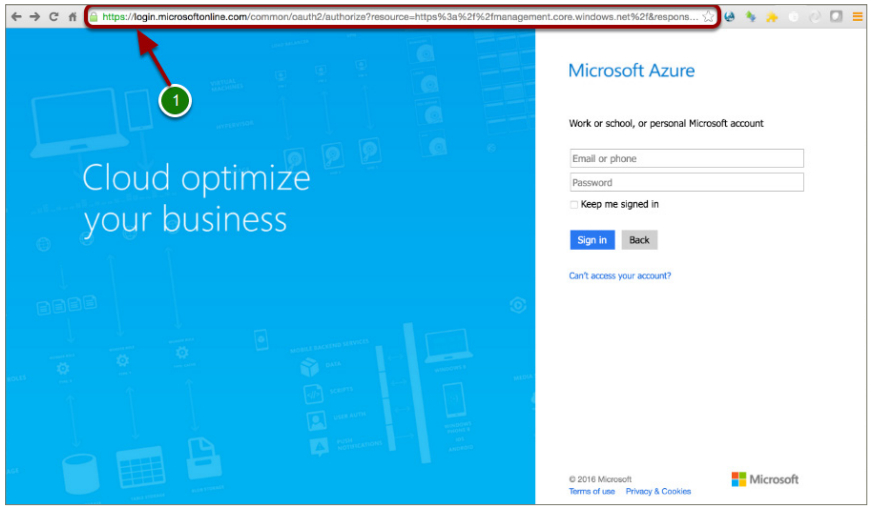
Step-by-Step Instructions to get the Fortinet FortiWeb Up and Running on Azure

The following section will take you through a step-by-step process in order to deploy Fortinet FortiWeb on Azure.

1. Log In to the Azure Portal

   You access the Azure portal using the following URL: https://portal.azure.com/

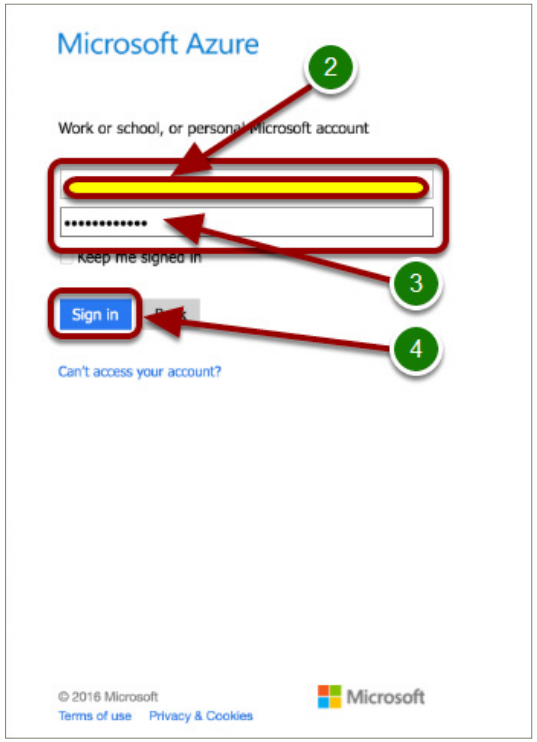
   The current Azure portal is the portal through which you will start creating and managing Azure services, such as the Fortinet FortiWeb Virtual Appliance. The Azure portal includes a dashboard that you can configure to work with and monitor the resources in your environment. The Azure portal lets you administer all of your Azure platform resources in a single location. The current Azure portal uses the Azure Resource Manager (ARM) template, although some classic model functionality is exposed through the new portal. The legacy or classic portal still is available for use, but the new portal has been released for general availability and is the portal you should use.



2. Enter User Credentials and Sign In

   Enter your user credentials:

   - Username: <Your Username> (2)
   - Password: <Your Password> (3)
   - Click "Sign in." (4)

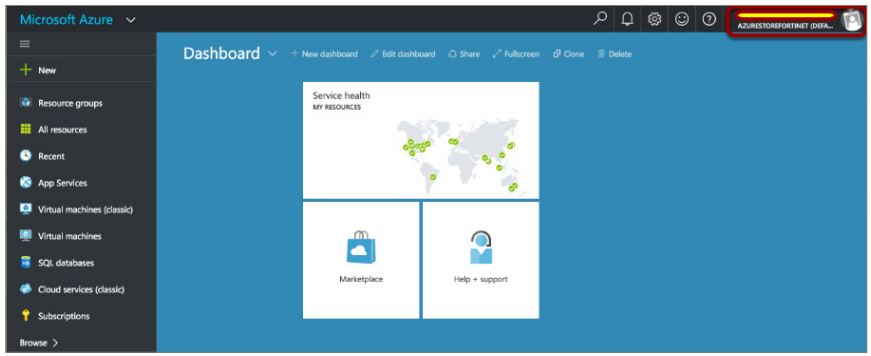


3. Successful Login to Azure

   Once you have successfully logged in to the Azure portal, you will observe the Microsoft Azure Dashboard.

   Note the following login details in the top right-hand corner of the Microsoft Azure Dashboard. If you click here, you will see options to:

   - Sign out
   - Change your password
   - View your permissions
   - View your bill

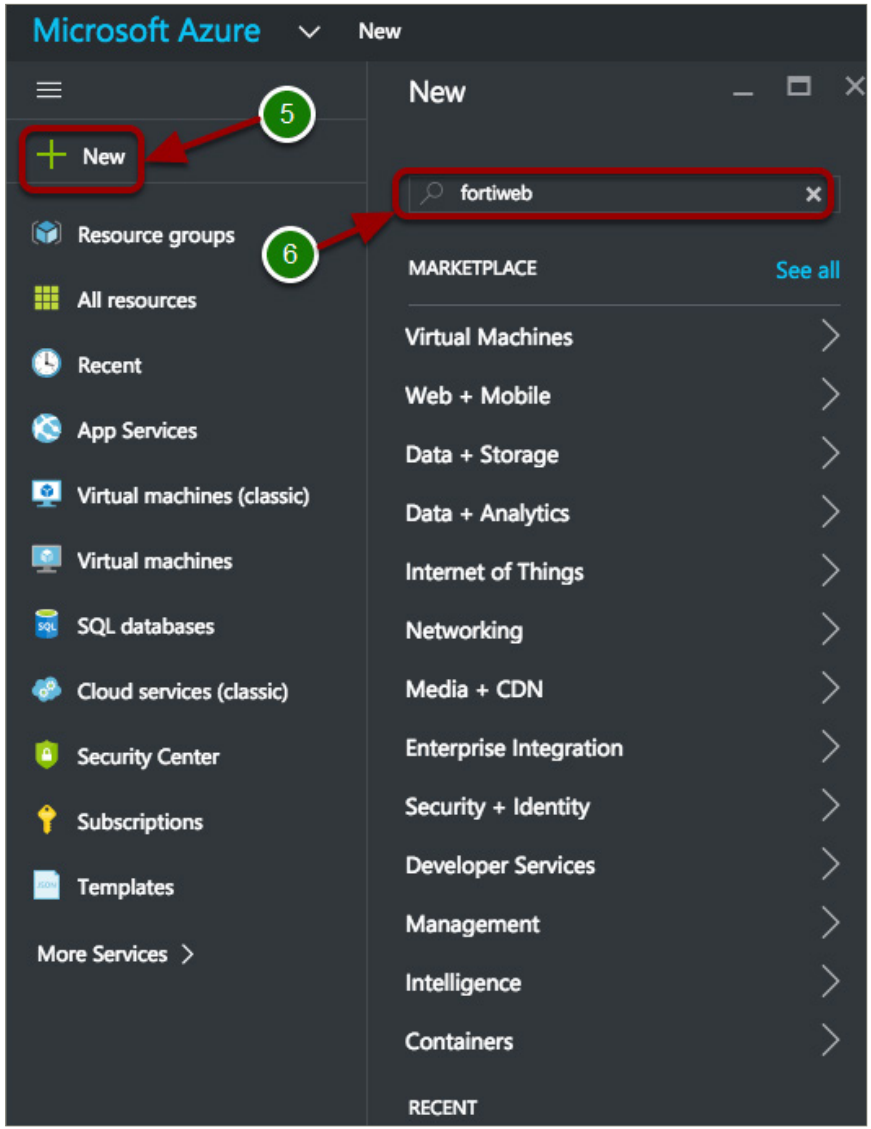


4. Creating the NEW Fortinet FortiWeb in the Azure Marketplace

   In the Microsoft Azure portal, follow these steps:

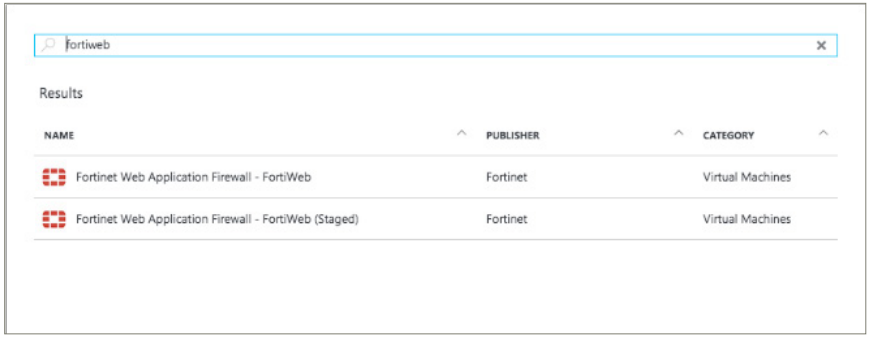
   - In the upper left-hand corner, click New (5).
   - In the New column, enter "fortiweb" in the "search the marketplace" and enter Return (6).

   NOTE: There are alternative ways of achieving the above; this is just one of the examples.



5. Fortinet Virtual Appliances Available in the Azure Marketplace

   You will now see something similar to this, which depicts the return of the "fortiweb" search results.



6. Select the Fortinet FortiWeb for Azure from the Azure Marketplace
   - Select the Fortinet Web Application Firewall - FortiWeb (7).

7. Select the Fortinet FortiWeb Deployment Model

   Once you have selected the Fortinet FortiWeb VM, you will automatically be taken to the Resource Manager Panel, where you can create a deployment model.

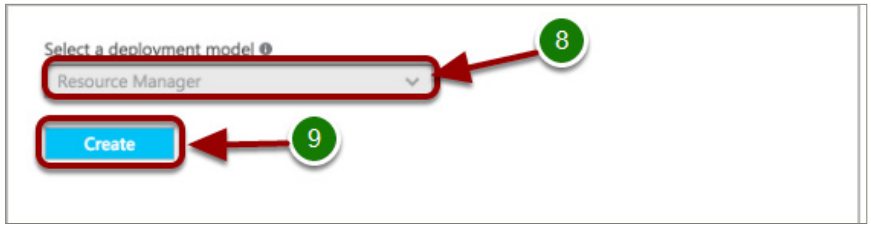
   - In the Select a deployment model, select the default Resource Manager (8).
   - Then click Create (9).

   NOTE: Though there is no option from the dropdown menu to select a different deployment model, this is where you would select the Classic deployment model option.

   Azure deployment models

   Azure provides two deployment models, the Classic model and the Azure Resource Manager (ARM) model. The foundation of each model is an application-programming interface (API), which is the Resource Manager API for ARM and the Service Management API for the classic model. Although developers can write software to interact with these APIs directly through the REST API, it is more common to interact with these APIs indirectly using the Azure portal, the Azure PowerShell on Windows, or the Azure Command-Line Interface (CLI) on a Windows, OS X, or Linux computer.

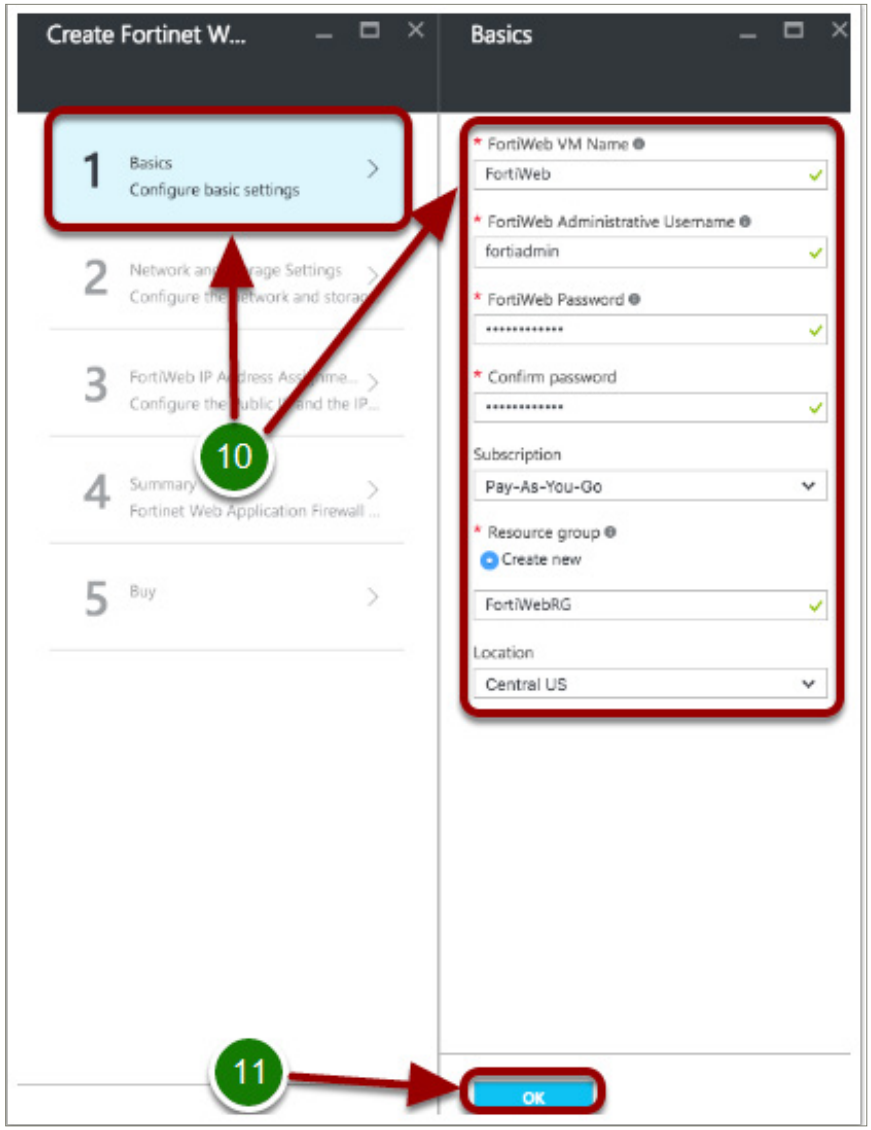
   In contrast to common belief, these two models are compatible with each other, but ARM simplifies the deployment and management of resources by managing them as a single resource group. Most newer resources support ARM, and eventually all resources will. However, how you create, configure, and manage Azure resources is different in these two models.



8. Configuring the FortiWeb VM - Basic

In the Configure basic settings panel (10), enter:

- **FortiWeb VM Name**—Enter the name of the FortiWeb Virtual Appliance. (Only alphanumeric characters are permitted, and the value must be between 1 and 15 characters.)
- **FortiWeb Administrative Username**—Enter the administrator username for the FortiWeb Virtual Appliance. (The administrator username for the FortiWeb Virtual Appliance cannot be "admin.") If you do enter "admin," you will get an error message stating that the specified username is NOT allowed. In addition to this, the username can NOT contain special characters.
- **FortiWeb Password**—Enter the administrator account password for the FortiWebVirtual Appliance. (The administrator account password MUST be between 6 and 72 characters, and MUST contain characters from at least three of the following groups: uppercase characters, lowercase characters, numbers, and special characters.)
- **Confirm password**—Re-enter the administrator account password for the FortiWeb Virtual Appliance.
- **Subscription**—The only available subscription for the FortiWeb Virtual Appliance in Azure is the Pay-As-You-Go subscription model, so just leave this as "default".
- **Resource group**—Enter the Resource group name, and note that only alphanumeric characters, periods, underscores, hyphens, and parentheses may be used. In addition to this, a Resource group name can NOT end with a "." (With Azure Resource Manager, everything you provision on Azure is a resource. You can put multiple resources into a resource group. Managing resource groups and creating and updating resource groups are the most common operations using Azure Resource Manager.)



NOTE: Recently Microsoft removed the ability to deploy into existing resource groups by marketplace; you will therefore need to create a FortiWeb Resource Group.

- **Location**—Select a location from the drop-down menu. The location refers to allowing you to administer all of your Azure platform resources in a single location.

Once you have confirmed that all the above settings are correct, click "OK." (11)

NOTE: If any of the values are incorrectly defined, you will see a "Red !"; otherwise, you will see a "Green ✓."

9. Configuring the FortiWeb VM - Network and Storage

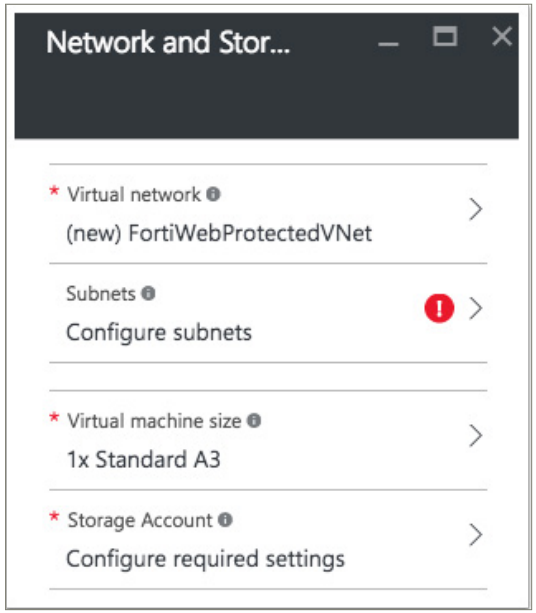
   Below you will find your virtual machine settings. It is important to note:

   - Storage account
   - Virtual network
   - Subnet
   - Public IP address, etc.

   These can be customized. You could, for example, change your Virtual Network (VNET) to 10.0.0.0/8 and select for Subnet 10.0.0.0/24 and 10.0.1.0/24 to be mapped inside/outside interfaces on the FortiWeb. This will be covered in detail later.

   At this time you could receive warnings of overlapping address space in different resource groups within your locations; however, this doesn't matter and they don't cross-connect.

   For purposes of clarity, we will use default values for the Standalone FortiWeb Quick Start Guide.



Configuring the FortiWeb VM - Network/Virtual Network

The first question that comes to mind about a virtual network (VNET) is why do we need a VNET? Well, the answer is a simple one and the basic principle here is that we need a VNET in order to be able to build a private network in the Azure Cloud.

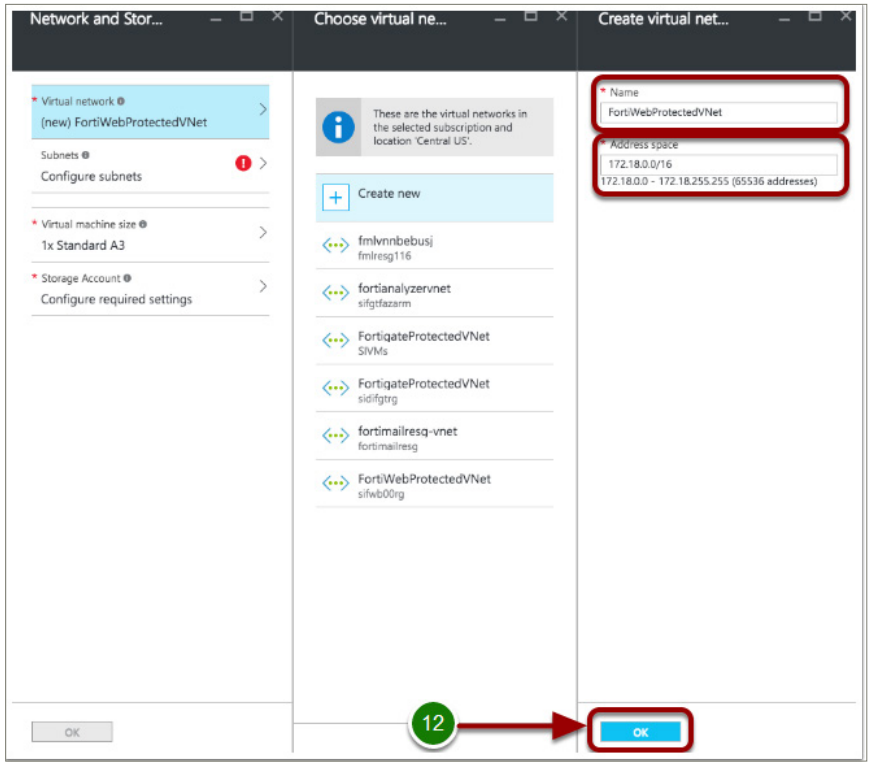
An Azure Virtual Network, which is also known or referred to as a VNET, is something that you only create in Microsoft Azure. The Azure Virtual Network enables virtual machines and the other resources that are part of the Azure Virtual Network to communicate with each other privately. It is the Azure Virtual Network that provides this communication function. If we did not have an Azure Virtual Network, or if a virtual machine was outside the Azure Virtual Network, then communication with other virtual machines would not be possible.

After you have selected the Virtual network settings, you will observe that you can either create a new VNET or select an existing one. If you select an existing VNET, it will need to have at least two subnets in order for the Fortinet FortiWeb to route between them. In a typical deployment, the “outside” subnet just connects the FortiWeb outside interface to the Azure Public Load Balancer and therefore does not need to be very large.

Here we created the Virtual Network Name of FortiWebProtectedVNet and the Address space of 172.18.0.0/16.

Click OK (12).

NOTE: No changes have been made here.



Configuring the FortiWeb VM - Network/Subnet

After you have selected the Subnets settings, you will also observe that we already have the following Subnets defined (13):

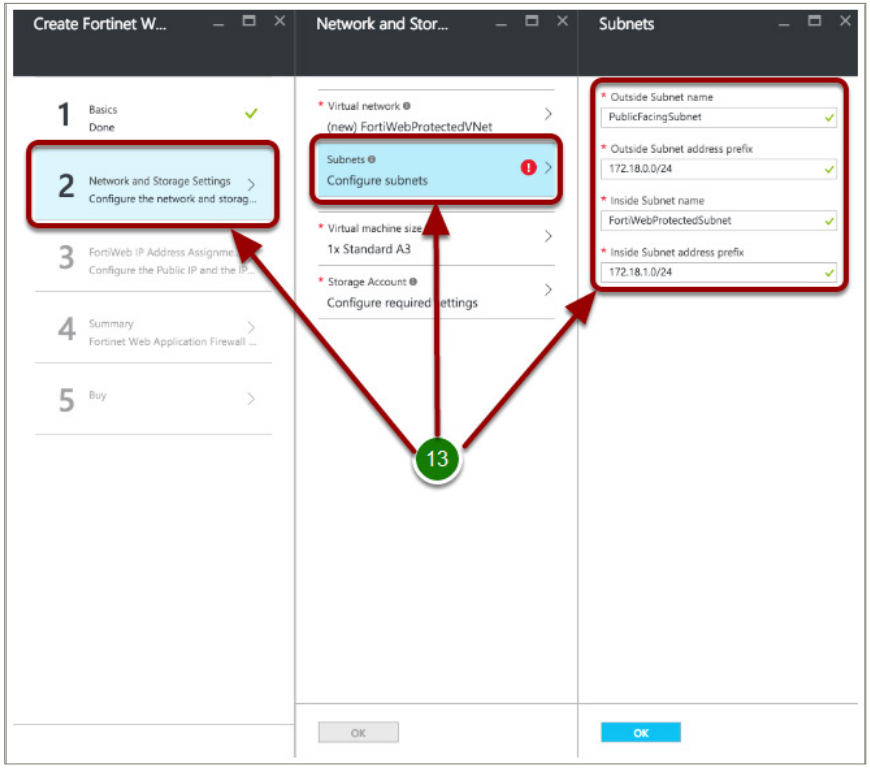
Subnet name: default

Outside Subnet address prefix: 172.18.0.0/24

Inside Subnet address prefix: 172.18.1.0/24

So how does the IP addressing work? When a virtual machine is deployed into a VNET, its internal IP address is assigned from the subnet you specify and is dependent on the order in which it was provisioned, unless a static IP has been specified. For example, the FortiWeb Subnet that was created uses the address prefix of 172.18.0.0/24. The first four IP addresses of each subnet are reserved. With this knowledge in hand, it is easy to deduce that the first IP address available in this subnet will be 172.18.0.5. Unless otherwise specified, a virtual machine will be assigned the next available IP address from the subnet to which it was assigned at provisioning time.

NOTE: No changes have been made here.



Configuring the FortiWeb VM - Size

In the Azure Marketplace, the FortiWeb virtual machines come in a variety of sizes, beginning with the A0 Standard up through D4 Standard. Each virtual machine size within each series has different limits for the amount of memory, number of NICs, maximum number of data disks, size of cache, and maximum IOPS and bandwidth.

Select the Virtual Machine Size Settings (14).

What are "A4 Standard" and "D4 Standard?" How do we select a VM by the number of vNICs?

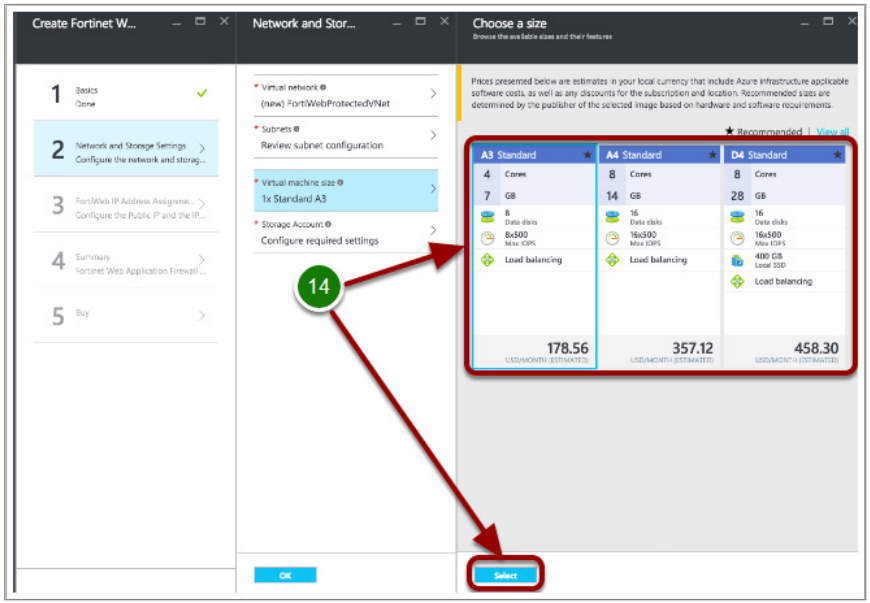
Sizing and performance benchmarking based on workloads or use cases are always challenging when selecting the particular "virtual machine size."

The "A4 Standard" and "D4 Standard," etc., are what are referred to as instance sizes. The instances are differentiated primarily on CPU and memory, although they also have different levels of support for multiple vNICs. For more information, please click on the following URL:

https://azure.microsoft.com/en-us/documentation/articles/virtual-machines-windows-sizes/

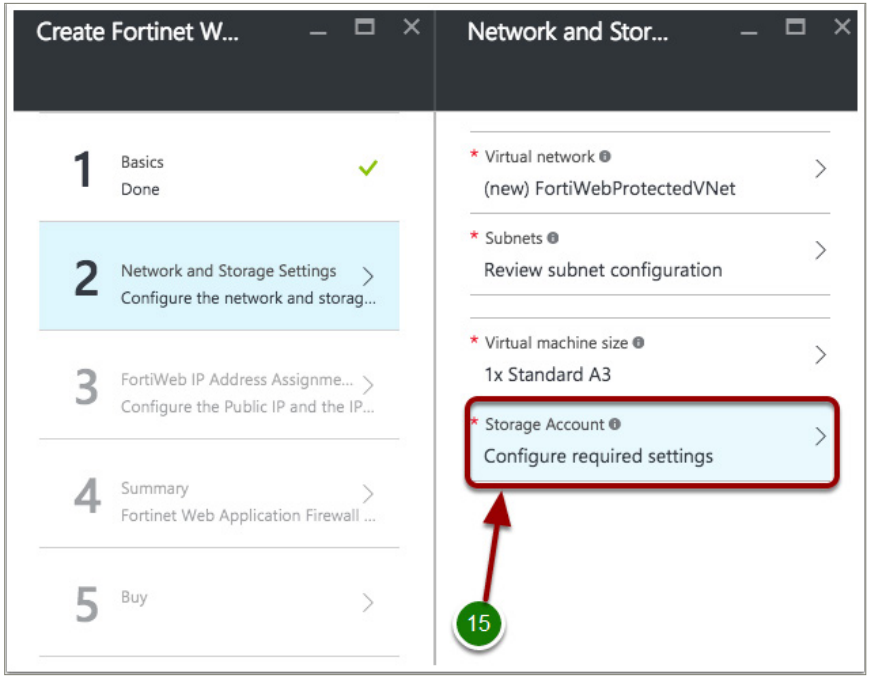
When you select a "virtual machine size," why do you not see the number of vNICs? From the "Choose a size" panel, you have no idea and would have to guess. The answer is that Azure has never prioritized multiple vNICs. So, the Azure Marketplace templates have a bias against them, and it's extremely difficult to create a variable number of vNICs. Fortinet's FortiWeb template facilitates the creation of two vNICs.

If you require more than one vNIC, you will need to deploy a custom template at this point. Please contact the Azure team (azuretech@fortinet.com) for assistance.



Configuring the FortiWeb VM Settings - Storage Account

Storage (15). Through the Storage workflow you can create a storage account associated with the newly created Fortinet FortiWeb VM.



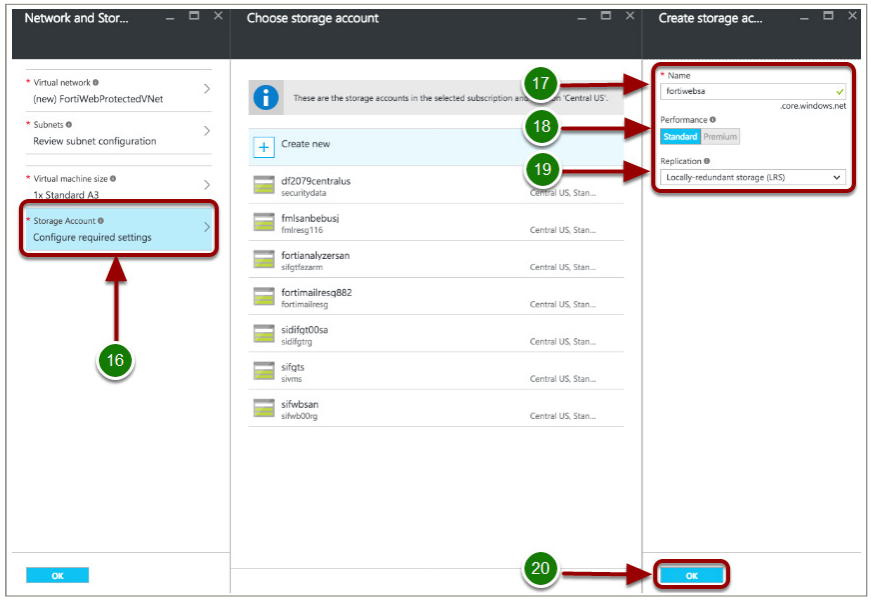
Without going into the details of the different types of storage available in Azure, it is important to note (there are few exceptions) that all storage types are created from an Azure Storage Account. The Azure Storage Account in turn determines certain characteristics for the storage, such as whether the storage is locally redundant or geo-redundant, and whether the storage is based on standard HDDs or SSDs.

You can either create a new storage account or select an existing one for the FortiWeb Virtual Appliance, but all resources should be in the same location (in this example: West Europe).

- Select the Storage Account settings (16).
- Enter a Storage Account Name (17). (This account name can contain lowercase characters and numbers, and must be between 3 and 24 characters.)
- Select the Performance (18). (In this instance only standard is available.)
- Select the Replication option you wish to use (19). There are two options available:
    1. Locally redundant storage (LRS)
    2. Geo-redundant storage (GRS)

Locally redundant storage (LRS) is where all data in the Azure Storage account replicates synchronously to three different storage nodes within the primary region that was chosen when creating the Azure Storage account.

Geo-redundant storage (GRS) is where every entity is replicated into two data centers.



The data in the Azure Storage Account is always replicated in order to ensure durability and high availability. Be aware that some settings cannot be changed after the storage account has been created.

- Select OK (20).

NOTE: We entered in the Name.

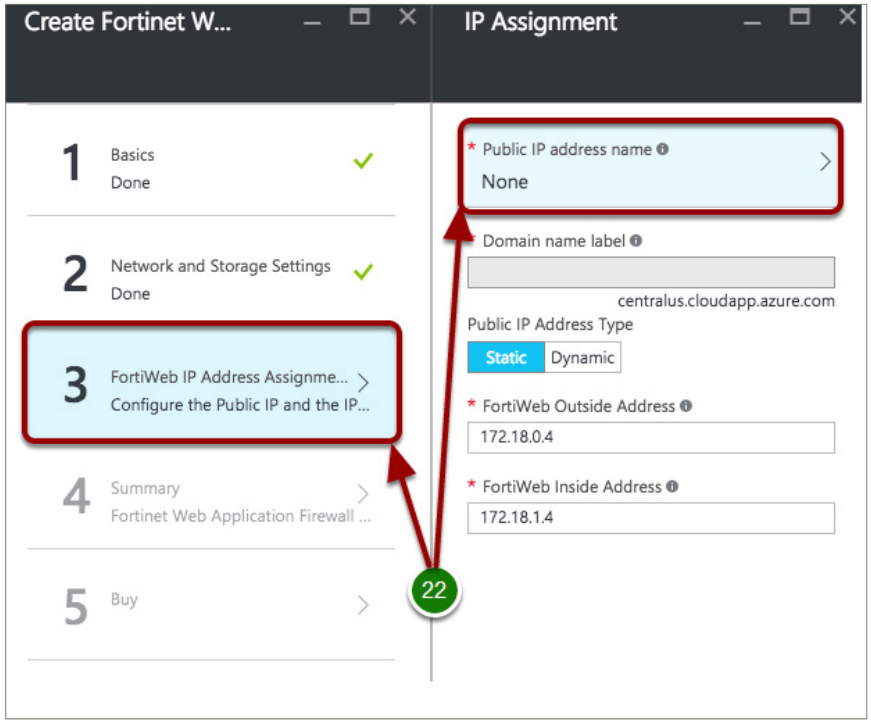
Configuring the FortiWeb Settings - OK

- Select OK (21) to finalize your Network and Storage Settings.

10. Configuring the FortiWeb VM - FortiWeb IP Address Assignments

    Configuring the FortiWeb IP Address Assignments has several sub-tasks, which will be covered in sequence below.

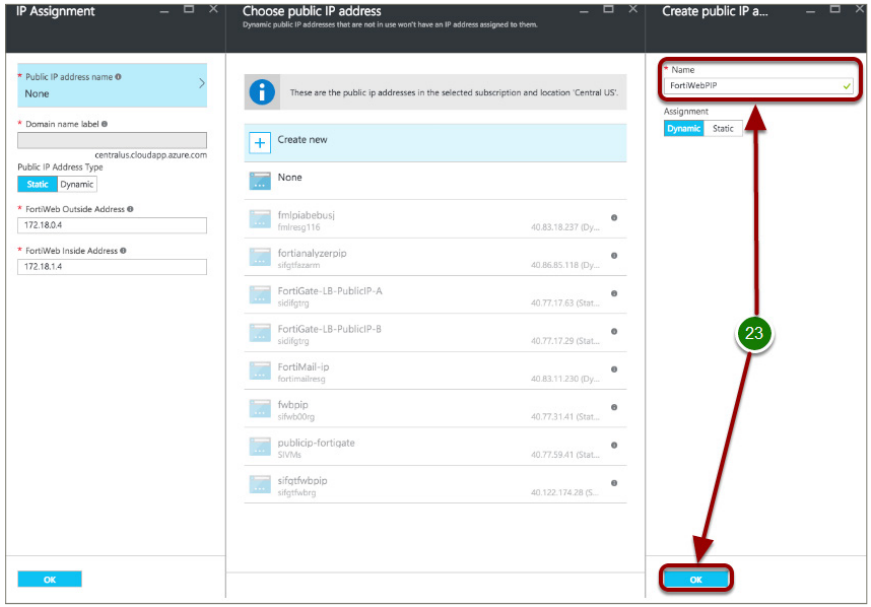
    - Click on Public IP address name (22).



Configuring the FortiWeb VM - FortiWeb IP Address Assignments: Name

- Here we are just going to enter the Name FortiWebPIP and Assignment Dynamic configuration and click OK. You could specify a static IP here within your subnet if you choose to do so (23).

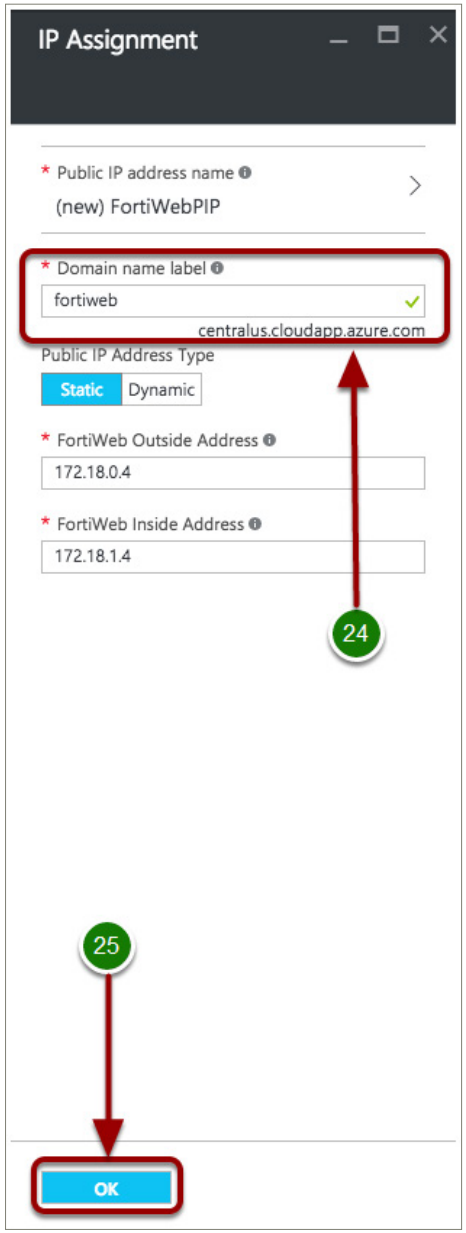
NOTE: No changes have been made here.



Configuring the FortiWeb VM - FortiWeb IP Address Assignments: Domain name label

- Enter your dns name (24) for the FortiWeb VM (e.g., fortiweb).
- Click OK (25).

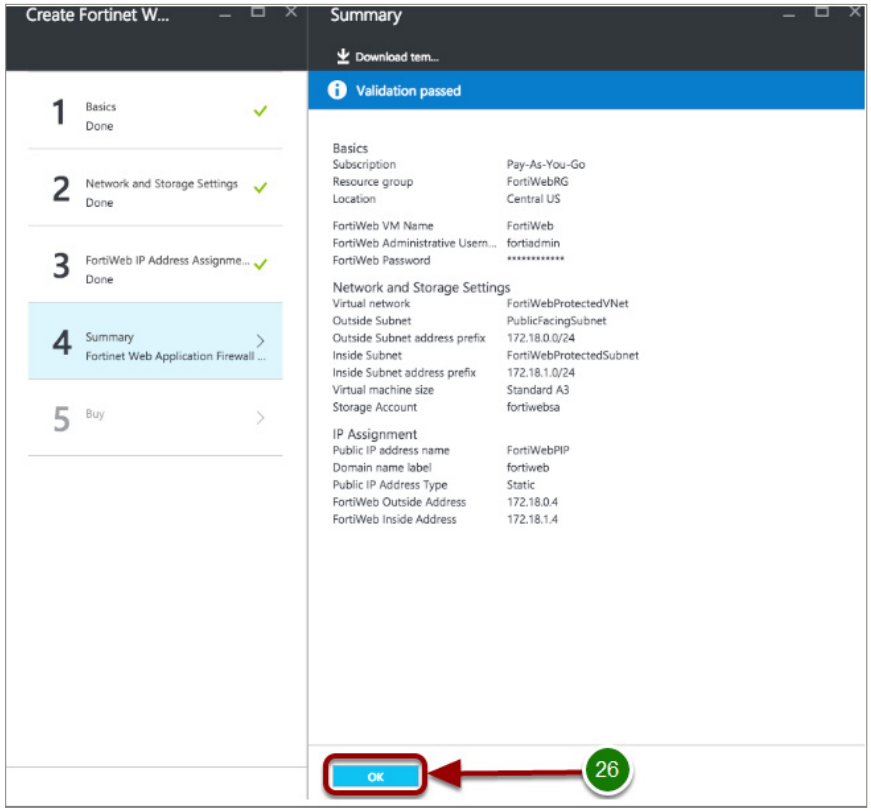
NOTE: FortiWeb Outside and Inside Addresses mapped as described earlier with first useable IP being 172.18.X.5.



11. Configuring the FortiWeb VM - Summary

    After selecting OK, a validation process will take place and your configuration will be validated. If successful, you will see "Validation passed."

    - Select OK (26).

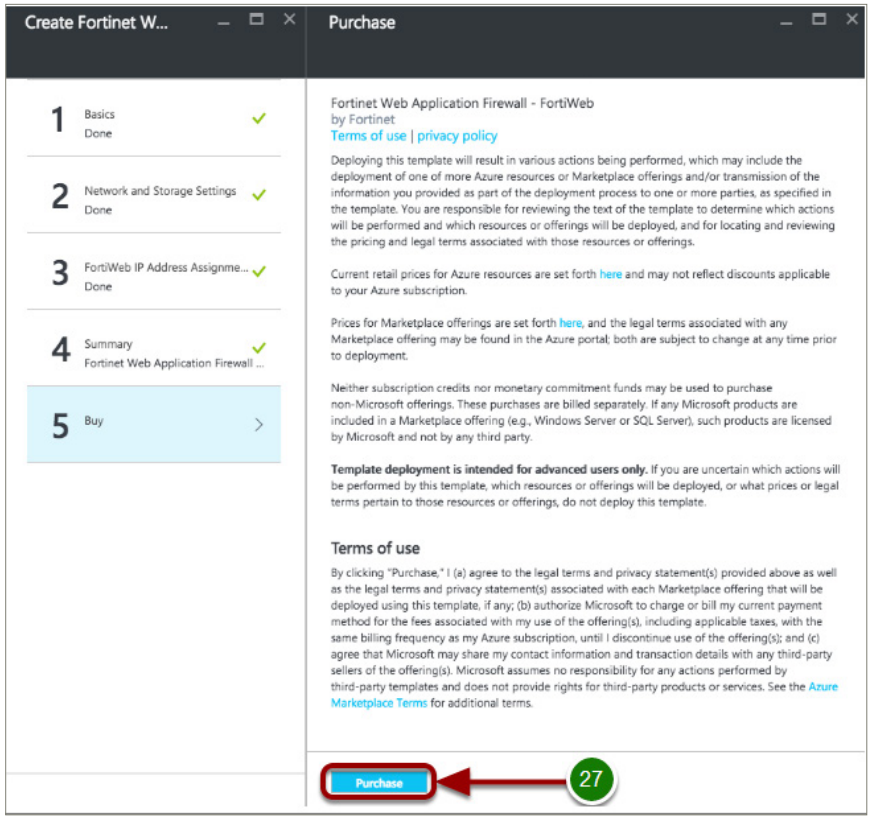


12. Configuring the FortiWeb VM - Buy

After the Fortinet FortiWeb VM Configuration has been completed, we now are required to select purchase.

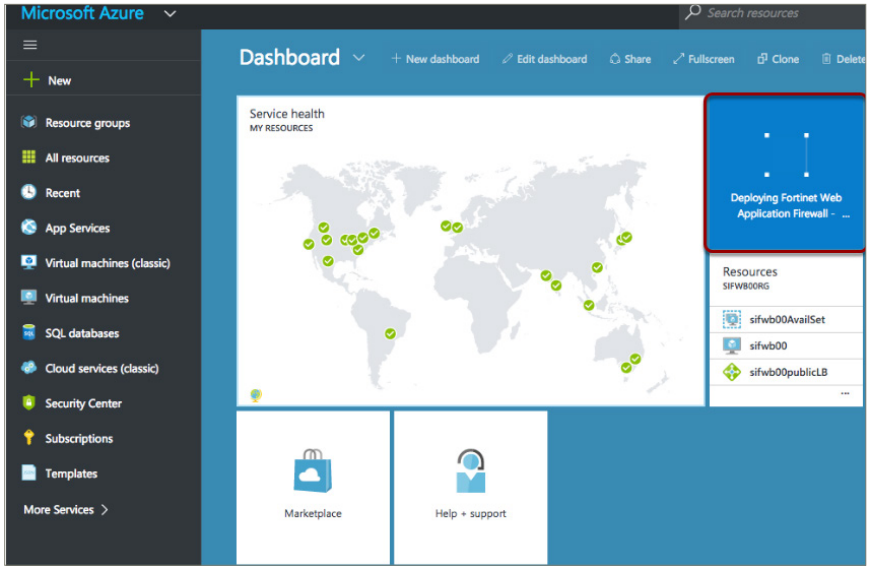
- Select Purchase (27).

NOTE: Purchase just means that you are going to be paying Azure for the virtual machine use time. You still must obtain a license separately from Fortinet, Inc.



13. Fortinet FortiWeb VM (Deploying)

After selecting Purchase, the Fortinet FortiWeb Single VM will be deployed. This process can take approximately 10 minutes to complete, but may vary depending on location and number of resources being requested.

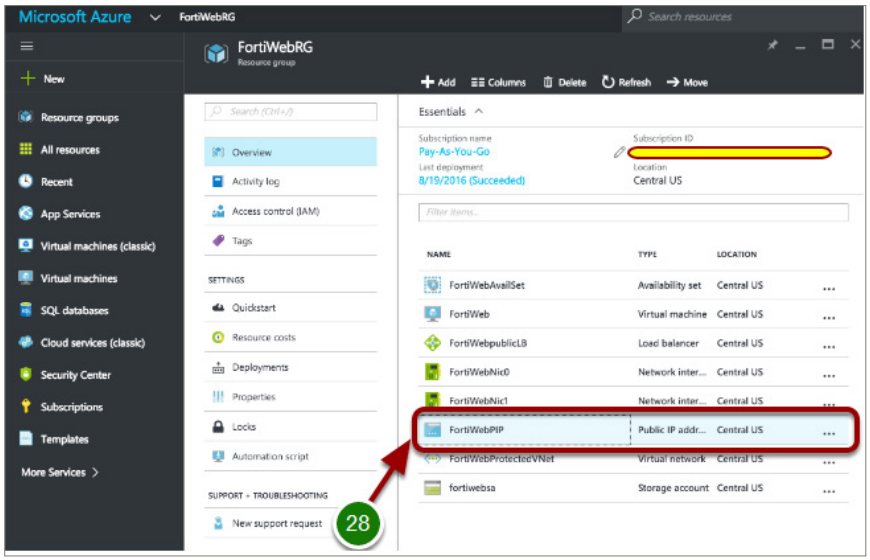


14. Connect to the FortiWeb Azure VM by public IP

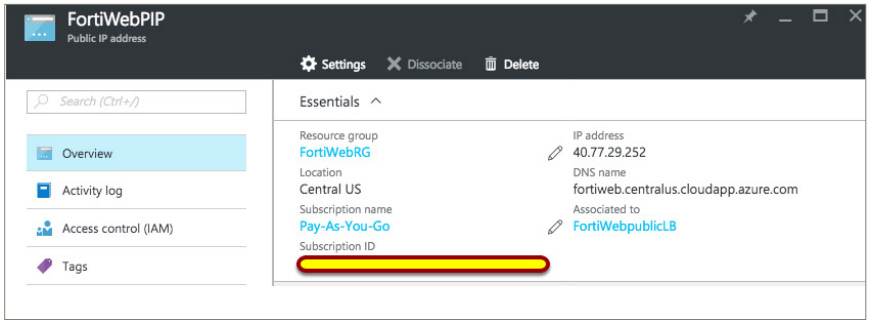
In order to be able to connect to the FortiWeb Public IP Address, we need know what this IP address is.

To accomplish this:

- Once again from the FortiWebRG Resource group, select FortiWebPIP (28).



This will expose the Public IP Address, which is: 40.77.29.252.



Connect to the FortiWeb Azure VM by public IP and change admin password

- SSH to our found Public IP Address (29), which is: 40.77.29.252

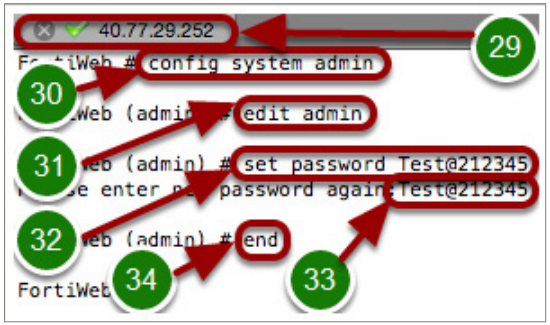
Recall in Step 8 we defined both the username and password, which are as follows and are required to connect to the FortiWeb Virtual Appliance UI:

- FortiWeb Administrative Username: fortiadmin
- FortiWeb Password: <the password you entered>

Once connected, enter the following:

- FortiWeb # **config system admin** (30)
- FortiWeb (admin) # **edit admin** (31)
- FortiWeb (admin) # **set password Test@212345** (32)
- Please enter new password again: **Test@212345** (33)
- FortiWeb (admin) # **end** (34)

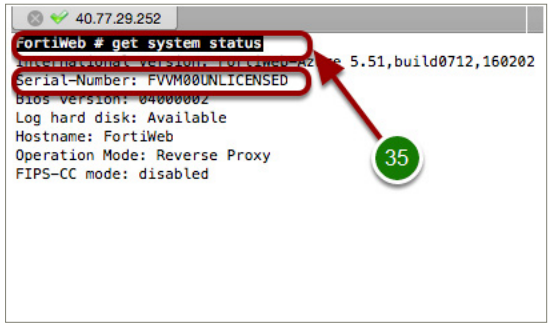
FortiWeb #



Connect to the FortiWeb Azure VM by public IP and view license

FortiWeb # **get system status** (35)

Once you have acquired an FWB-AZ BYOL, you will be able to upload it via the GUI.

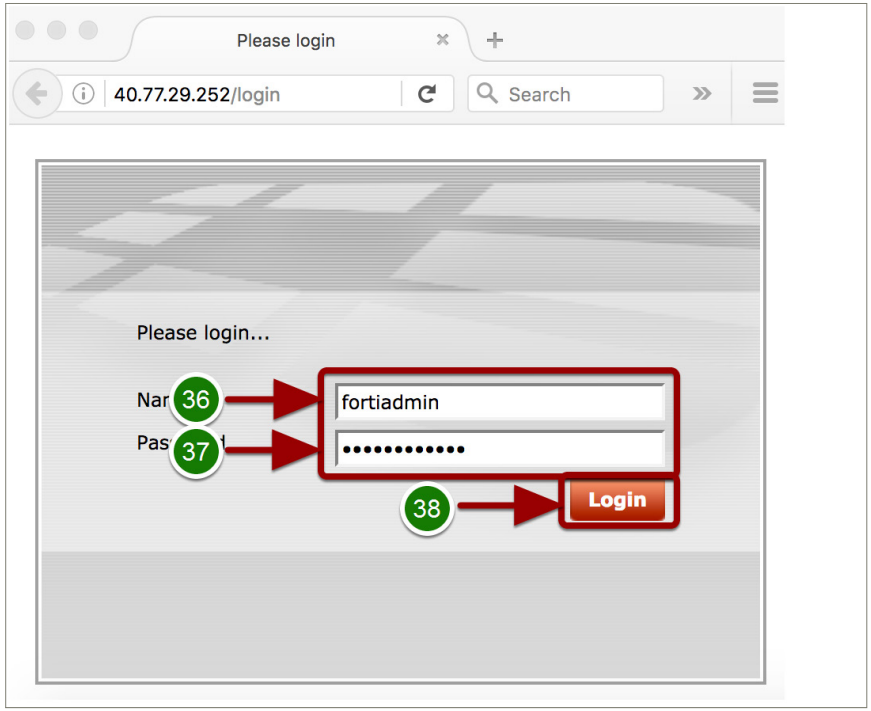


Connect to the FortiWeb Azure VM by public IP via HTTPS

HTTPS to our found Public IP Address, which is 40.77.29.252

Recall in Step 8 we defined both the username and password, which are as follows and are required to connect to the FortiWeb Virtual Appliance UI:

- FortiWeb Administrative Username (36): fortiadmin
- FortiWeb Password (37): <the password you entered>
- Click Login (38).



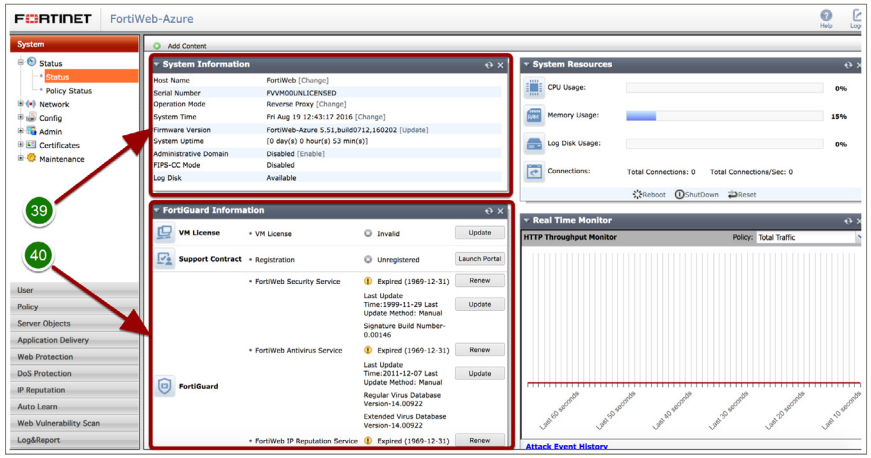
Now that you are connected and positioned on the System Status page, you can see widgets with basic information such as:

System Information (39)

- Host Name
- Operational Mode
- System Time
- Firmware Version
- Uptime
- Administrative Domains, etc.

FortiGuard Information (40)

- VM License
- Support Contract
- FortiGuard

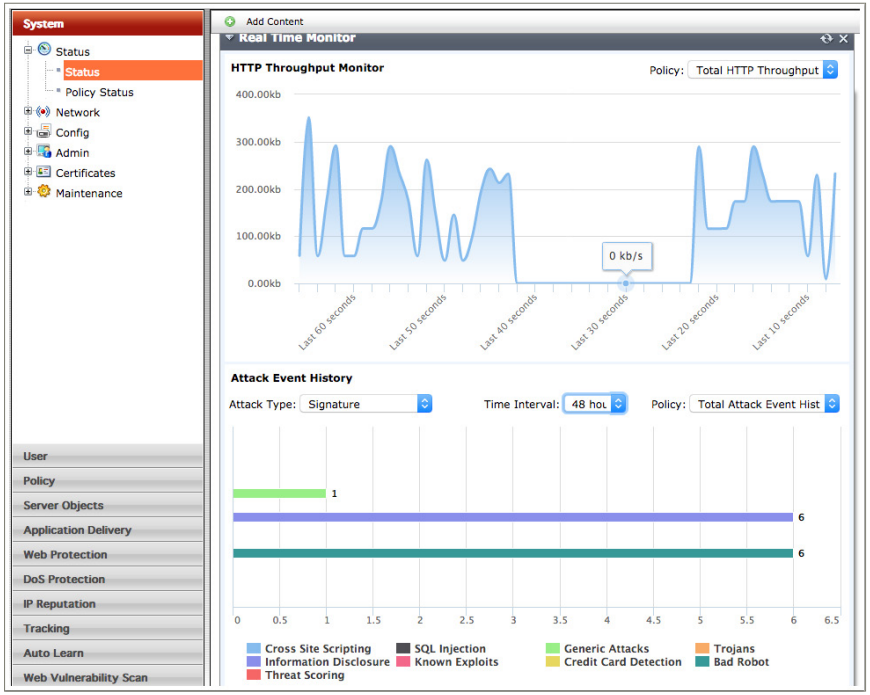


15. Verify Functionality

With a web server behind FortiWeb, you will configure:

- Server Objects
- Server Pools
- Server Policies
- Protection Profiles

Once this has been completed, common tools like OWASP Top 10 Zapper can be run to generate traffic or look for exploits.



Support

For more in-depth instructions, please refer to http://docs.fortinet.com/ for administration guides or email your support questions to azuretech@fortinet.com.

v1.0 09.07.16